NIST SP 800-37 Rev 2
NIST Risk Management Framework for Information Systems and Organizations

NIST Risk Management Framework for Information Systems and Organizations

NIST SP 800-37 Version 2 Issued December 2018

SCOPE:

- Mandatory for federal information systems, which are discrete sets of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether such information is in digital or non-digital form. Information resources include information and related resources, such as personnel, equipment, funds, and information technology.
- Can be applied to any type of nonfederal organization (e.g., business, industry, academia

NIST Risk Management Framework for Information Systems and Organizations

PURPOSE: Provide guidelines for managing security and privacy risks and applying the Risk Management Framework (RMF) to information systems and organizations

Guidelines are developed to:

- Ensure that managing system-related security and privacy risk is consistent with the mission and business objectives of the organization and risk management strategy established by the senior leadership through the risk executive (function)
- Achieve privacy protections for individuals and security protections for information and information systems through the implementation of appropriate risk response strategies
- Support consistent, informed, and ongoing authorization decisions, reciprocity, and the transparency and traceability of security and privacy information
- Facilitate the integration of security and privacy requirements and controls into the enterprise architecture, SDLC processes, acquisition processes, and systems engineering processes
- Facilitate the implementation of the *Framework for Improving Critical Infrastructure Cybersecurity* within federal agencies

NIST Risk Management Framework for Information Systems and Organizations

Some Key Definitions:

- **Authorization Package**: The essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the provision of a designated set of common controls. At a minimum, the authorization package includes an executive summary, system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones
- **Control Assessment**: The testing or evaluation of the controls in an information system or an organization to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization
- **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
- **Organization**: An entity of any size, complexity, or positioning within an organizational structure (e.g., federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or as appropriate, any of their operational elements)
- **Privacy Control**: The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks

NIST Risk Management Framework for Information Systems and Organizations

Some Key Definitions:

- **Risk**: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence
- **Risk Assessment**: The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system
- **Risk Management:** The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time
- **Security**: A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach
- **Security Control**: The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information
- **System**: Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions

NIST Risk Management Framework for Information Systems and Organizations

NIST Risk Management Framework Steps:

- **Prepare** to execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk
- **Categorize** the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss
- **Select** an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk
- **Implement** the controls and describe how the controls are employed within the system and its environment of operation
- **Assess** the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements
- **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable
- **Monitor** the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system

NIST Risk Management Framework for Information Systems and Organizations

PREPARE Tasks – Organizational Level

- **PROJECT MANAGEMENT ROLES**: Identify and assign individuals to specific roles associated with security and privacy risk management
- **RISK MANAGEMENT STRATEGY**: Establish a risk management strategy for the organization that includes a determination of risk tolerance
- **RISK ASSESSMENT—ORGANIZATION:** Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis
- **ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES** (Optional): Establish, document, and publish organizationally-tailored control baselines and/or Cybersecurity Framework Profiles
- **COMMON CONTROL IDENTIFICATION:** Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems
- **IMPACT-LEVEL PRIORITIZATION** (Optional): Prioritize organizational systems with the same impact level
- **CONTINUOUS MONITORING STRATEGY—ORGANIZATION:** Develop and implement an organization-wide strategy for continuously monitoring control effectiveness

NIST Risk Management Framework for Information Systems and Organizations

PREPARE Tasks – System Level

- **MISSION OR BUSINESS FOCUS**: Identify the missions, business functions, and mission/business processes that the system is intended to support
- **SYSTEM STAKEHOLDERS**: Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system
- **ASSET IDENTIFICATION:** Identify assets that require protection
- **AUTHORIZATION BOUNDARY**: Determine the authorization boundary of the system
- **INFORMATION TYPES:** Identify the types of information to be processed, stored, and transmitted by the system
- **INFORMATION LIFE CYCLE**: Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system
- **RISK ASSESSMENT—SYSTEM:** Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis

NIST Risk Management Framework for Information Systems and Organizations

PREPARE Tasks – System Level (cont'd)

- **REQUIREMENTS DEFINITION:** Define the security and privacy requirements for the system and the environment of operation
- **ENTERPRISE ARCHITECTURE:** Determine the placement of the system within the enterprise architecture
- **REQUIREMENTS ALLOCATION:** Allocate security and privacy requirements to the system and to the environment of operation
- **SYSTEM REGISTRATION:** Register the system with organizational program or management offices

NIST Risk Management Framework for Information Systems and Organizations

CATEGORIZE Tasks

- **SYSTEM DESCRIPTION**: Document the characteristics of the system
- **SECURITY CATEGORIZATION**: Categorize the system and document the security categorization results
- **SECURITY CATEGORIZATION REVIEW AND APPROVAL:** Review and approve the security categorization results and decision

NIST Risk Management Framework for Information Systems and Organizations

SELECT Tasks

- **CONTROL SELECTION**: Select the controls (from NIST SP 800-53) for the system and the environment of operation
- **CONTROL TAILORING**: Tailor the controls selected for the system and the environment of operation
- **CONTROL ALLOCATION:** Allocate security and privacy controls to the system and to the environment of operation
- **DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS:** Document the controls for the system and environment of operation in security and privacy plans
- **CONTINUOUS MONITORING STRATEGY—SYSTEM:** Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy
- **PLAN REVIEW AND APPROVAL:** Review and approve the security and privacy plans for the system and the environment of operation

NIST Risk Management Framework for Information Systems and Organizations

IMPLEMENT Tasks

- **CONTROL IMPLEMENTATION**: Implement the controls in the security and privacy plans
- **UPDATE CONTROL IMPLEMENTATION INFORMATION**: Document changes to planned control implementations based on the "as-implemented" state of controls

NIST Risk Management Framework for Information Systems and Organizations

ASSESS Tasks

- **ASSESSOR SELECTION**: Select the appropriate assessor or assessment team for the type of control assessment to be conducted
- **ASSESSMENT PLAN**: Develop, review, and approve plans to assess implemented controls
- **CONTROL ASSESSMENTS**: Assess the controls in accordance with the assessment procedures described in assessment plans
- **ASSESSMENT REPORTS**: Prepare the assessment reports documenting the findings and recommendations from the control assessments
- **REMEDIATION ACTIONS:** Conduct initial remediation actions on the controls and reassess remediated controls
- **PLAN OF ACTION AND MILESTONES:** Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports

NIST Risk Management Framework for Information Systems and Organizations

AUTHORIZE Tasks

- **AUTHORIZATION PACKAGE**: Assemble the authorization package and submit the package to the authorizing official for an authorization decision
- **RISK ANALYSIS AND DETERMINATION**: Analyze and determine the risk from the operation or use of the system or the provision of common controls
- **RISK RESPONSE:** Identify and implement a preferred course of action in response to the risk determined
- **AUTHORIZATION DECISION**: Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable
- **AUTHORIZATION REPORTING:** Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk

NIST Risk Management Framework for Information Systems and Organizations

MONITOR Tasks

- **SYSTEM AND ENVIRONMENT CHANGES**: Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system
- **ONGOING ASSESSMENTS**: Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy
- **ONGOING RISK RESPONSE:** Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones
- **AUTHORIZATION PACKAGE UPDATES**: Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process
- **SECURITY AND PRIVACY REPORTING:** Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy
- **ONGOING AUTHORIZATION:** Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable
- **SYSTEM DISPOSAL:** Implement a system disposal strategy and execute required actions when a system is removed from operation